



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/802,485	03/09/2001	Burton S. Kaliski JR.	RSA-052	5894
<div>7590 Eric L. Prah, Esq. HALE AND DORR LLP 60 State Street Boston, MA 02109</div>				
			EXAMINER KLIMACH, PAULA W	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 12/12/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/802,485

Applicant(s)

KALISKI, BURTON S.

Examiner

Paula W. Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4-20,31,38-41 and 43-51 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,4-20,31,38-41 and 43-51 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 10/17/07
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application
- ☐ Other: _____

DETAILED ACTION***Response to Amendment***

This office action is in response to amendment filed on 10/17/07. The amendment filed on 10/17/07 have been entered and made of record. Therefore, presently pending claims are 1-2, 4-20, 31, 38-41, and 43-51.

Response to Arguments

Applicant's arguments filed 10/17/07 have been fully considered but they are not persuasive because of following reasons.

Applicant argued Jones does not disclose a multi-party secure computation protocol between a client and a server to compute a third secret. This is persuasive, however, Spelman teaches that a multi-party secure computation protocol between a client and a server. The client of Spelman (merchant) contains a reencryptor that encrypts the message sent from the client using the server's (merchant acquirer's) key.

The applicant argues further neither client (merchant) nor the server (merchant acquirer) of Spelman has any involvement in computing $C[GSO]_{k1}$; $D[PI]_{k2}$; $E[k1, \dots]_R$; $E[k2, \dots]_R$, which the examiner treats as the third secret of the claims. This is not found persuasive. The claims do not indicate that either the client or the server are involved in the computation of the third secret. The claims indicate that the client obtains the third secret without determining the server secret. In the system of Spelman the third secret is sent to the client (merchant) wherein the client obtains the client secret (GPO). In addition the claim language indicates that the server cannot feasibly determine the client secret and cannot determine the third secret. In the system

Art Unit: 2135

of Spelman the server (merchant acquirer) cannot feasibly determine the client secret and the third secret. As shown in figure 2 and 3 the server cannot calculate the third secret and the GSO.

The applicant argued further that there is no motivation for one of ordinary skill in the art to combine the systems of Spelman and Jones in the way the examiner proposes because the consumer is the only party involved in computing the so-called third secret and the client and server of the claims play no role in generating the so-called third secret. The applicant argues further that there would be no motivation for including these components in Jones systems.. This is not found persuasive. As indicated in the discussion above, the claim language for the application does not indicate that the client and server calculate the third secret. In fact, there is nothing in the claim language that indicates where the third secret is calculated.

Rejections for claims 1-2, 4-20, 31, 38-41, and 43-48 are maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-2, 4-7, 9-11, 14-18, 31, 38-41, and 43-48, are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones (5,623,637) in view of the article by Spelman et al. (5,638,445).

In reference to claims 1, 38, and 47, Jones discloses a multi-party system with a remote computer (server) and a host personal computer (client). The system of Jones after

Art Unit: 2135

authenticating, provides to the client by the device the encrypted secrets (column 8 lines 2-67 in combination with column 9 lines 22-36).

Although Jones discloses a method of key distribution, Jones does not disclose a protocol wherein the client has a client secret and the server has a server secret used to compute a third secret from the client and server secret and the server cannot feasibly determine the client secret and cannot feasibly determine the third secret.

Spelman teaches a method for blind encryption (title). Spelman a protocol wherein the client (merchant) has a client secret (GSO) and the server (merchant acquirer) has a server secret (PI) used to compute a third secret ($C[GSO]_{k1}$; $D[PI]_{k2}$; $E[k1, \dots]_R$; $E[k2, \dots]_R$) from the client and server secret, wherein the protocol is implemented so that the client obtains the third secret (Fig. 1 arrow with data point to part 20) and cannot feasibly determine the server secret (PI is encrypted by $k2$ which is encrypted by the recryptor's key R), and the server cannot feasibly determine the client secret (GSO is encrypted by $k1$ which is encrypted by the recryptor's key and is not sent to the merchant acquirer) and cannot feasibly determine the third secret (the merchant acquirer only has access the PI which is encrypted using $k2$ that the merchant acquirer has access to). The encrypted secrets are capable of being decrypted using a decryption key derived from the third secret (Fig. 3). The multi-party secure computation protocol implemented between the client and the server is the only multi-party computation protocol that is implemented in generating the third secret and the decryption key derived from the third secret (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the blinding encryption system of Spelman in the system of Jones. One of

Art Unit: 2135

ordinary skill in the art would have been motivated to do this because blind encryption is used to protect against snooping by the service (column 1 lines 34-36).

In reference to claim 4, wherein the client secret comprises at least one of a PIN, a password, and biometric information (column 8 lines 52-67).

In reference to claim 9, wherein the authenticating step comprises authenticating the client based on at least one of a PIN, a password, and biometric information (column 8 lines 52-67).

In reference to claims 10, wherein authenticating comprises authenticating the client based on a secret other than the first secret (column 8 lines 52-67).

In reference to claim 43 Spelman discloses a system wherein at the client, using the client secret to compute client information and then sending the client information to the server; at the server, using the client information and the server secret to compute intermediate data and sending the intermediate data to the client; and at the client, deriving the third secret from the intermediate data (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the blinding encryption system of Spelman in the system of Jones. One of ordinary skill in the art would have been motivated to do this because blind encryption is used to protect against snooping by the service (column 1 lines 34-36).

In reference to claims 2, 41, and 48 wherein the third secret is derived from the intermediate data by use of one of a key derivation function and a hash function. The polynomial is the key derivation function (Fig. 1).

Art Unit: 2135

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the blinding encryption system of Spelman in the system of Jones. One of ordinary skill in the art would have been motivated to do this because blind encryption is used to protect against snooping by the service (column 1 lines 34-36).

In reference to claims 11 wherein authenticating comprises using an authentication secret derived from the third secret (column 9 lines 1-21).

In reference to claim 14, wherein the encrypted secrets comprise a private key of a public/private key pair used for asymmetric cryptography (Fig. 3).

In reference to claim 15, wherein the encrypted secrets comprise a signature key used for creating a digital signature.

Jones does not expressly disclose encrypted secrets comprise a signature key used for creating a digital signature.

However Spelman discloses the key distribution for creating digital signatures (column 5 lines 55-62).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the blinding encryption system of Spelman in the system of Jones. One of ordinary skill in the art would have been motivated to do this because blind encryption is used to protect against snooping by the service (column 1 lines 34-36).

In reference to claim 16, wherein authenticating comprises authenticating the client based on a secret other than the first secret, so that the user provides different information to access the device and access the signature key column 9 lines 1-21.

In reference to claim 17, The method of claim 1 wherein the encrypted secrets comprise a secret key used for symmetric cryptography (column 9 lines 49-60).

In reference to claim 31 the method further comprising deriving the decryption key from the third secret; and decrypting the encrypted secrets using the decryption key (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the blinding encryption system of Spelman in the system of Jones. One of ordinary skill in the art would have been motivated to do this because blind encryption is used to protect against snooping by the service (column 1 lines 34-36).

In reference to claim 39, further comprising transmitting, to the first server by the network server, verification that the user has authenticated successfully.

Although Jones discloses the authentication of the host (client) to the remote computer (server), Jones does not disclose transmitting, to the first server by the network server, verification that the user has authenticated successfully. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send verification to the client from the server that is the network server. One of ordinary skill in the art would have been motivated to do this because in the case that the authentication is successful, the information would be sent to the host computer, however if authentication is not successful the host computer could use the verification transmission to make corrections and try again.

In reference to claim 40, wherein the network server is a web server and wherein the client is a web browser. The server of Jones is a server on the network, therefore a network server. The common use of the network described by Jones (Fig. 1) is for the internet, therefore the server would be a web server and the client a browser.

Art Unit: 2135

In reference to claims 5 and 44, Jones does not disclose a blind function evaluation protocol used to derive the intermediate data from the secret data.

Spelman discloses a merchant device deriving an intermediate message from a secret message sent by the consumer. The merchant device uses blind encryption to determine the intermediate data (Fig. 1 in combination with column 6 lines 15-30).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to blind the secret data as disclosed by Spelman in the system disclosed Jones. One of ordinary skill in the art would have been motivated to do this because it would facilitate communication between devices in the case that the keys have not been exchanged yet.

In reference to claims 6, wherein the security of the blind function evaluation protocol is based on the problem of extracting roots modulo a composite.

Jones does not disclose the user of a blind function.

Spelman discloses the user of a blind encryption function wherein the evaluation protocol is based on the problem of extracting roots modulo a composite (column 6 lines 31-44).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to blind the secret data as disclosed by Spelman in the system disclosed Jones. One of ordinary skill in the art would have been motivated to do this because it would facilitate communication between devices in the case that the keys have not been exchanged yet.

In reference to claims 7 and 45-46, wherein the security of the blind function evaluation protocol uses discrete logarithms.

Jones does not disclose the user of a blind function.

Art Unit: 2135

Spelman discloses the user of a blind encryption function wherein the evaluation protocol uses the discrete logarithm problem (column 6 lines 31-44).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to blind the secret data as disclosed by Spelman in the system disclosed Jones. One of ordinary skill in the art would have been motivated to do this because it would facilitate communication between devices in the case that the keys have not been exchanged yet.

In reference to claim 18, wherein the encrypted secrets comprise at least one unit of digital currency.

Jones does not disclose the encrypted secrets comprising at least one unit of digital currency.

Spelman discloses the data being sent from a merchant to a merchant acquirer, therefore the information includes digital currency with visa information (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send digital currency as suggested by Spelman in the system disclosed Jones. One of ordinary skill in the art would have been motivated to do this because communication of currency requires enhanced security to prevent theft.

In reference to claim 49-51, the system wherein the multi-party secure computation protocol comprises the client and the server providing their respective secrets as input to respective protocol operations that jointly calculate the third secret as a function of the client and server secrets (Fig. 2). The GSO and PI are provided as input to calculate $(C[GSO]_{k1}; D[PI]_{k2}; E[k1, \dots]_R; E[k2, \dots]_R)$, the third secret. Wherein the GSO is the secret input of the client and

Art Unit: 2135

therefore provided by the client and PI is the secret of the server and therefore provided by the server. The protocol is illustrated by Figure 2.

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jones and Spelman as applied in claim 1 and further in view of Schneier.

In reference to claim 8, wherein the authenticating step comprises authenticating the client based on a time-dependent code. Jones and Spelman do not expressly disclose the client authenticating based on a time-dependent code.

Schneier discloses the use of the timestamp during authentication (page 61). The information used during authentication is then time-dependent.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a time stamp during authentication as in Schneier in the system disclosed by Jones. One of ordinary skill in the art would have been motivated to do this because the time stamp would prevent replay attacks.

Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones and Spelman as applied in claim 1 and further in view of Richard et al (5,922,074).

In reference to claim 12 wherein the device comprises at least one of a file server, a directory server, a key server, a PDA, a mobile telephone, a smart card, and a desktop computer.

Jones and Spelman do not expressly disclose the device comprising at least one of a file server, a directory server, a key server, a PDA, mobile telephone, a smart card, and a desktop computer.

Art Unit: 2135

Richard discloses a system that includes a directory server from which the client authenticates to gain access (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the client to a directory server as in Richard in the system of Jones. One of ordinary skill in the art would have been motivated to do this because the directory includes sensitive information that requires increased security.

In reference to claim 13, wherein the device comprises at least one secure data store, the device-requiring authentication before allowing the client access to the data store.

Although Jones discloses a system wherein the device requires authentication before allowing the client access to the data, Jones does not expressly disclose a system wherein the device comprises at least one secure data store.

Richard discloses a system wherein the client authenticates itself to a server that stores information or services (column 6 lines 21-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the client to a server that stores information or services as in Richard in the system of Jones. One of ordinary skill in the art would have been motivated to do this because the directory includes sensitive information that requires increased security.

Claims 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones and Spelman as applied to claim 43 and further in view of Brunsting et al (6,505,164).

In reference to claim 19, further comprising the step of verifying that the client has not exceeded a predetermined number of unsuccessful attempts to obtain the intermediate data.

Art Unit: 2135

Jones and Spelman do not disclose a system that maintains a count of the number of unsuccessful attempt to authenticate a system.

Brunsting discloses a system that maintains a count of the number of unsuccessful attempts at accessing account information (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a count of the number of unsuccessful attempts as in Brunsting in the system of Jones. One of ordinary skill in the art would have been motivated to do this because it would increase security by monitoring the activity that may be malicious.

In reference to claim 20, wherein the verifying step further comprises: transmitting a challenge code to the client; and receiving the result of a cryptographic operation using the challenge code as an input and using a cryptographic key derived from the encrypted secret (Jones Fig. 2).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2135

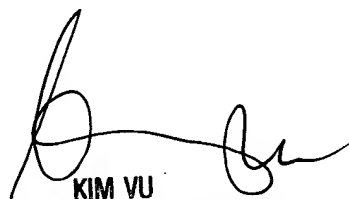
however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Friday, December 07, 2007



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 21